JOURNAL OF ALGEBRA 22, 201–210 (1972)

Orders in Hopf Algebras*

RICHARD GUSTAVUS LARSON

Department of Mathematics, University of Illinois at Chicago Circle Chicago, Illinois 60680

Communicated by David Buchsbaum

Received February 22, 1971

Number-theoretic techniques are very useful in studying the representation theory of finite groups. In this paper we attempt to introduce such techniques into the representation theory of finite-dimensional semisimple involutory Hopf algebras over a number field. We consider Hopf algebras which contain an integral Hopf algebra order, and study the relation between the structure of the Hopf algebra and the number-theoretic properties of its orders.

Let H be a finite-dimensional semisimple involutory Hopf algebra. An element $\Lambda \in H$ is called a left integral if $h\Lambda = \epsilon(h)\Lambda$ for all $h \in H$. It is known [5, 6] that there exist left integrals in H for which $\epsilon(\Lambda) \neq 0$. Let A be an order in H, and let L be the ideal of all left integrals in A. The ideal $\epsilon(L)$ gives much information on the structure of H and A. It plays a role similar to that played by the order of the group in discussing the representation theory of a finite group. In fact it always is a divisor of dim H. More specifically, let A^* be the dual order to A in H^*, and let L^* be the ideal of left integrals in A^*. We prove that $\epsilon(L)\,\epsilon(L^*)$ is the ideal generated by dim H. A is a separable algebra if and only if $\epsilon(L) = R$. If B is an order containing A, and M is the ideal of left integrals contained in B, we show that $(\epsilon(L)\,\epsilon(M)^{-1}) \cdot (B/A) = 0$. In particular, if $\epsilon(L) = \epsilon(M)$, it follows that $B = A$. We then prove the following generalization of a theorem of Frobenius: the degree of any absolutely irreducible representation of H divides $\epsilon(L)$. If H is the group algebra of a group G, and A is the integral group ring, then $\epsilon(L) = (|\,G\,|)$, and this gives Frobenius' theorem. If G has a normal abelian subgroup N, then it is possible to construct an order for which $\epsilon(L) = ([G : N])$, in which case our result gives us a theorem of Ito. This

* This research was supported by National Science Foundation grant GP-9584. Much of the work in Section 4 was done while the author was attending a meeting at the Mathematisches Forschungsinstitut Oberwolfach. He wishes to express his gratitude to the Institute for their hospitality.

proof of Ito's theorem is interesting in that it does not use induction on subgroups. Finally, we show that a Hopf algebra over a number field which contains a separable order must be commutative.

Throughout this paper we will freely use the results of [5, 6, 4]. A good exposition of the relevant material in the first two papers can be found in [7].

1. Hopf Algebras and Orders

Let R be a Dedekind domain. By a *bialgebra* over R, we mean an R-algebra A with unit which is a finitely generated projective R-module, together with R-algebra homomorphisms $\delta : A \to A \otimes_R A$ and $\epsilon : A \to R$ satisfying

$$(I \otimes \delta)\delta = (\delta \otimes I)\delta$$

and

$$(I \otimes \epsilon)\delta = (\epsilon \otimes I)\delta = I.$$

We will follow the usual convention [7, pp. 10–12] and denote $\delta(a)$ by $\sum a_{(1)} \otimes a_{(2)}$, $(I \otimes \delta)\,\delta(a)$ by $\sum a_{(1)} \otimes a_{(2)} \otimes a_{(3)}$, etc. If there exists an R-module map $\gamma : A \to A$ satisfying

$$\epsilon(a)1 = \sum a_{(1)}\gamma(a_{(2)}) = \sum \gamma(a_{(1)})\, a_{(2)} ,$$

we will call A a *Hopf algebra*. A is called *involutory* if $\gamma^2 = I$.

If X is a finitely generated projective R-module, denote the R-module $\hom_R(X, R)$ by X^*. Note that $X^{**} \cong X$; if Y is also a finitely generated projective R-module, then $(X \otimes_R Y)^* \cong X^* \otimes_R Y^*$. If A is a Hopf algebra over R, A^* is a Hopf algebra over R, called the dual Hopf algebra to A. $A^{**} \cong A$ as Hopf algebras.

Let F be the field of quotients of a Dedekind domain R, and let H be a finite-dimensional Hopf algebra over F. An *R-order* of H is a Hopf algebra A over R which is finitely generated and projective as an R-module, such that $A \otimes_R F \cong H$. If A is an R-order of H, we will usually identify A with its image in H under the isomorphism. Note that under this identification $A^* = \hom_R(A, R)$ is identified with the set of elements $p \in H^* = \hom_F(H, F)$ for which $p(A) \subset R$.

Let H be a finite-dimensional Hopf algebra over F. A *left integral* in H is an element $\Lambda \in H$ such that $h\Lambda = \epsilon(h)\Lambda$ for all $h \in H$. It is shown in [5] that the set of all left integrals in H is an ideal of dimension 1 over F. Since any Hopf algebra A over R is an order of $A \otimes_R F$, it follows that A contains nonzero left integrals. Let L denote the set of left integrals in A. Then L is a two-sided ideal in A.

If Λ is an element of L such that $L = R\Lambda$, we call Λ a *nonsingular* left integral in A. If there exists a nonsingular left integral in A it is determined up to multiplication by a unit in R.

If $h \in H$ and $p \in H^*$, denote $\sum h_{(1)} p(h_{(2)})$ by $p{>}h$ and $\sum p(h_{(1)}) h_{(2)}$ by $h{<}p$. Note that $q(p{>}h) = qp(h)$ and $q(h{<}p) = pq(h)$ for all $q \in H^*$. Let A be an R-order of H. If $h \in A$ and $p \in A^*$, the $p{>}h$, $h{<}p \in A$.

LEMMA 1.1. *Let R be a Dedekind domain, let A be a Hopf algebra over R, and let L be the ideal of left integrals in A. Then the map*

$$A^* \otimes_R L \to A$$

defined by

$$p \otimes h \mapsto h{<}\gamma(p), \qquad p \in A^*, \quad h \in L,$$

is an R-module isomorphism.

Proof. It is enough to show that the map $(A^* \otimes_R L) \otimes_R R_P \to A \otimes_R R_P$ is an isomorphism for all primes $P \subset R$. Since $(A^* \otimes_R L) \otimes_R R_P \cong (A^* \otimes_R R_P) \otimes_{R_P} (L \otimes_R R_P) \cong (A \otimes_R R_P)^* \otimes_{R_P} (L \otimes_R R_P)$, and $A \otimes_R R_P$ is a Hopf algebra over R_P with dual $(A \otimes_R R_P)^*$ and ideal of left integrals $L \otimes_R R_P$, and since R_P is a principal ideal domain, the Lemma follows from the main theorem of [5].

COROLLARY 1.2. *Let R be a Dedekind domain, and let A be a Hopf algebra over R. Then a left integral $\Lambda \in A$ is nonsingular if and only if the map*

$$A^* \to A$$

defined by

$$p \mapsto \Lambda{<}\gamma(p)$$

is an R-module isomorphism.

Proof. The *only if* portion of the Corollary follows from the Lemma.

If. Let L be the ideal of left integrals in A. Then $L = \{q\Lambda \mid q \in I\}$ where I is some fractional ideal in F, the field of quotients of R. We know that $A = L{<}\gamma(A^*) = (I\Lambda){<}\gamma(A^*) = I(\Lambda{<}\gamma(A^*)) = IA$. This implies that $I = R$, so $L = R\Lambda$, and Λ is a nonsingular left integral. Q.E.D.

The following lemma is immediate.

LEMMA 1.3. *Let R be a Dedekind domain, and let A be a Hopf algebra over R. If A^* is a free R-module with basis $\{p_i\}$, and $\Lambda \in A$ is a left integral, then Λ is nonsingular if and only if the matrix $(p_i p_j(\Lambda))$ is invertible over R.*

2. Left Integrals and Duality

In this section we show that if A is an R-order in a finite-dimensional semisimple involutory Hopf algebra H, if L is the ideal of left integrals in A and L^* is the ideal of left integrals in A^*, then $\epsilon(L)\,\epsilon(L^*) = (\dim H)R$. This result can be thought of as a more precise arithmetic version of Theorem 4.3 of [4]. We then show that an involutory Hopf algebra A over R is separable if and only if $\epsilon(L) = R$.

We call a semisimple Hopf algebra H over F *split* if every irreducible module M over H is absolutely irreducible, that is, if $M \otimes_F E$ is irreducible over $H \otimes_F E$ for all field extensions E/F. If H is any finite-dimensional semisimple Hopf algebra over F, there exists a finite extension E/F such that $H \otimes_F E$ is split.

If H is split over F, we can carry through the development of the character theory as in [4]; all the results found there will hold for H. If $\chi \in H^*$ is an irreducible character of H, we will denote the degree of χ by d_χ.

Lemma 2.1. *Let H be a finite-dimensional semisimple involutory Hopf algebra which is split over the field F, and let H^* be its dual Hopf algebra. Let Λ be a nonsingular left integral in H, and let Λ^* be a nonsingular left integral in H^*. Then*

$$\epsilon(\Lambda)\,\Lambda^* = \Lambda^*(\Lambda) \sum d_\chi \chi,$$

where the sum ranges over the distinct irreducible characters of the algebra H.

Proof. Let $\Lambda_0 = \epsilon(\Lambda)^{-1}\Lambda$. Then Λ_0 is a nonsingular left integral in H with $\epsilon(\Lambda_0) = 1$. The proof of Proposition 4.1 of [4] shows that

$$\Lambda^* = \Lambda^*(\Lambda_0) \sum d_\chi \chi.$$

The lemma now follows from this.

Proposition 2.2. *Let R be a Dedekind domain with field of quotients F. Let H be a finite-dimensional semisimple involutory Hopf algebra over F, let A be an R-order in H, and let A^* be the dual R-order in H^*. If L is the ideal of left integrals in A and L^* is the ideal of left integrals in A^*, then*

$$\epsilon(L)\,\epsilon(L^*) = (\dim H)R.$$

Proof. It is sufficient to show that for each prime $P \subset R$, $\epsilon(L)\,\epsilon(L^*)\,R_P = (\dim H)\,R_P$. Note that $L \otimes_R R_P$ is the ideal of left integrals in the R_P-order $A \otimes_R R_P$ and $L^* \otimes_R R_P$ is the ideal of left integrals in the R_P-order $A^* \otimes_R R_P = (A \otimes_R R_P)^*$. Since $\epsilon(L)\,\epsilon(L^*)\,R_P = \epsilon(L \otimes_R R_P)\,\epsilon(L^* \otimes_R R_P)$, it is sufficient to show that $\epsilon(L \otimes_R R_P)\,\epsilon(L^* \otimes_R R_P) = (\dim H)\,R_P$. In other words, we may assume (replacing R by R_P) that R is a discrete valuation ring. In particular, since R is a principal ideal domain, A has a nonsingular integral Λ and A^* has a nonsingular integral Λ^*. That is, $L = R\Lambda$ and $L^* = R\Lambda^*$. By Proposition 7 of [5], we may assume $\Lambda^*(\Lambda) = 1$. We will show that $\epsilon(\Lambda)\,\epsilon(\Lambda^*) = (\dim H)1$.

Let E/F be a finite field extension which splits the algebra H, and let S be the integral closure of R in E. Λ is a nonsingular integral in $A \otimes_R S$ and Λ^* is a nonsingular integral in $A^* \otimes_R S = (A \otimes_R S)^*$. Thus we may assume (replacing R by S) that H is split. By Lemma 2.1,

$$\epsilon(\Lambda)\,\Lambda^* = \Lambda^*(\Lambda) \sum d_\chi \chi.$$

This implies

$$\begin{aligned}\epsilon(\Lambda)\,\epsilon(\Lambda^*) &= \Lambda^*(\Lambda) \sum d_\chi \epsilon(\chi) \\ &= \sum d_\chi^2 = (\dim H)1.\end{aligned}$$

This completes the proof of the Proposition.

The following example shows that we cannot drop the hypothesis that H is involutory and semisimple. Consider the Hopf algebra H generated over the rational numbers by g and t, with $\delta(g) = g \otimes g$, $\epsilon(g) = 1$, and $\delta(t) = 1 \otimes t + t \otimes g$, $\epsilon(t) = 0$, subject to the relations $g^2 = 1$, $t^2 = 0$, and $gt + tg = 0$. It can be shown that H is a four-dimensional Hopf algebra with basis $\{1, g, t, gt\}$. The antipode of H is given by $\gamma(1) = 1$, $\gamma(g) = g$, $\gamma(t) = gt$, $\gamma(gt) = -t$. The antipode is of order four; so H is not involutory. H is not semisimple; its radical has basis $\{t, gt\}$. It can be shown that $\Lambda = t + gt$ is a left integral in H and that the functional Λ^* defined by $\Lambda^*(1) = 0$, $\Lambda^*(g) = 0$, $\Lambda^*(t) = 1$, $\Lambda^*(gt) = 0$ is a left integral in H^*. (This Hopf algebra is a homomorphic image of the example given on pp. 89–90 of [7].) Now consider the $\mathbf{Z}$-order A in H spanned by $\{1, g, t, gt\}$. It can be shown that the element Λ described above is a nonsingular left integral in A, and that Λ^* is a nonsingular left integral in A^*. Therefore in this case $\epsilon(L)\,\epsilon(L^*) = 0 \neq 4\mathbf{Z} = (\dim H)\mathbf{Z}$.

COROLLARY 2.3. *Let R be a Dedekind domain with field of quotients F. Let H be a finite-dimensional semisimple involutory Hopf algebra over F, let A be an R-order in H, and let A^* be the dual R-order to A in H^*. Suppose that the characteristic of F does not divide the dimension of H. If A has a nonsingular left integral Λ, then A^* has a nonsingular left integral Λ^* such that* $\epsilon(\Lambda)\,\epsilon(\Lambda^*) = (\dim H)1$.

Proof. By the Proposition, $\epsilon(\Lambda)\,\epsilon(L^*) = (\dim H)R$, so there exists $\Lambda^* \in L^*$ with $\epsilon(\Lambda)\,\epsilon(\Lambda^*) = (\dim H)1 \neq 0$. It is easily checked that Λ^* is a nonsingular left integral in A^*.

Let A be a Hopf algebra over the Dedekind domain R. If $a \in A$, denote by $R(a)$ the R-endomorphism of A defined by $bR(a) = ba$. Consider the element $T^* \in A^*$ defined by $T^*(a) = \mathrm{Tr}(R(a))$ for all $a \in A$. By Proposition 9 of [5], if A is involutory, then T^* is a left integral.

LEMMA 2.4. *Let H be a semisimple involutory Hopf algebra over the field F. If Λ, Λ^* are left integrals in H, H^* satisfying $\Lambda^*(\Lambda) = 1$, then $T^* = \epsilon(\Lambda)\Lambda^*$.*

Proof. Let E be a finite extension of F which splits H. Replacing H by $H \otimes_F E$, we can assume that H is split. Since T^* is a left integral in H^*, by Lemma 2.1,

$$\epsilon(\Lambda)\, T^* = T^*(\Lambda) \textstyle\sum d_x \chi.$$

It is clear that $\sum d_x \chi$ is the trace of the right regular representation, that is, $\sum d_x \chi = T^*$. Therefore, $\epsilon(\Lambda) = T^*(\Lambda)$. Since Λ^* is a nonzero left integral, $T^* = t\Lambda^*$ for some $t \in F$. Now $\epsilon(\Lambda) = T^*(\Lambda) = t\Lambda^*(\Lambda) = t$ since $\Lambda^*(\Lambda) = 1$. Therefore, $T^* = \epsilon(\Lambda)\Lambda^*$. Q.E.D.

PROPOSITION 2.5. *Let A be an involutory Hopf algebra over the Dedekind domain R, let A^* be the dual Hopf algebra, and let L be the ideal of left integrals in A. Then the following statements are equivalent:*

1. *A is a separable R-algebra*
2. *T^* is a nonsingular left integral in A^**
3. *$\epsilon(L) = R$.*

Proof. A is separable if and only if $A \otimes_R R_P$ is separable for every maximal ideal $P \subset R$ (Proposition 4.5 of [1]). T^* is a nonsingular left integral if and only if it is a nonsingular left integral in $A^* \otimes_R R_P$ for every maximal ideal $P \subset R$. $\epsilon(L) = R$ if and only if $\epsilon(L \otimes_R R_P) = R_P$ for every maximal ideal $P \subset R$. Therefore we can replace R by R_P and assume that R is a discrete valuation ring.

The equivalence of (1) and (2) is known; see the first Corollary to Proposition 9 in [5]. Let F be the field of quotients of R. Either of (2) or (3) implies that $H = A \otimes_R F$ is semisimple. Since we are working over a discrete valuation ring, by [5] we can find nonsingular left integrals Λ, Λ^* in A, A^* with $\Lambda^*(\Lambda) = 1$. By Lemma 2.4, $T^* = \epsilon(\Lambda)\Lambda^*$, so $RT^* = \epsilon(L)L^*$. The equivalence of (2) and (3) now follows. Q.E.D.

3. A RELATION BETWEEN ORDERS

Suppose A, B are orders in a finite-dimensional semisimple Hopf algebra. Denote the ideals of left integrals by L_A, L_B. In this section we show that if

$A \subset B$, then $(\epsilon(L_A)\,\epsilon(L_B)^{-1}) \cdot (B/A) = 0$. In particular, if $A \subset B$ and $\epsilon(L_A) = \epsilon(L_B)$, then $A = B$.

PROPOSITION 3.1. *Let R be a Dedekind domain with quotient field F. Let H be a finite-dimensional semisimple Hopf algebra over F, and let A, B be R-orders in H. Let L_A be the ideal of left integrals in A, and let L_B be the ideal of left integrals in B. If $B \supset A$, then $\epsilon(L_A)B \subset \epsilon(L_B)A$.*

Proof. To prove the Proposition, it is enough to show that $\epsilon(L_A)\, R_P B \subset \epsilon(L_B)\, R_P A$ for all primes $P \subset R$. Therefore, replacing R by R_P and A, B by $A \otimes_R R_P$, $B \otimes_R R_P$, respectively, we may assume that R is a discrete valuation ring. In particular, R is a principal ideal domain. Applying the main theorem of [5], we see that A has a nonsingular left integral Λ_A and B has a nonsingular left integral Λ_B. Let $\{b_i{}^*\}$ be an R-basis for B^*. Given $a^* \in A^*$, we can write $a^* = \sum_i q_i b_i{}^*$, with $q_i \in F$. We will show that $\epsilon(\Lambda_A)\, q_i \in \epsilon(\Lambda_B)R$. Since $B^* \subset A^*$, $a^* b_j{}^*(\Lambda_A) \in R$. Since Λ_B is a nonsingular left integral in B, the matrix $(b_i{}^* b_j{}^*(\Lambda_B))$ is invertible and its inverse (u_{ij}) has entries in R. Therefore

$$\begin{aligned}
\epsilon(\Lambda_A)\, q_i &= \epsilon(\Lambda_A) \sum_{j,k} q_k b_k{}^* b_j{}^*(\Lambda_B)\, u_{ji} \\
&= \epsilon(\Lambda_A) \sum_{j} a^* b_j{}^*(\Lambda_B)\, u_{ji} \\
&= \epsilon(\Lambda_B) \sum a^* b_j{}^*(\Lambda_A)\, u_{ji} \in \epsilon(\Lambda_B)R.
\end{aligned}$$

Therefore,

$$\epsilon(\Lambda_A)\, a^* = \sum_i \epsilon(\Lambda_A)\, q_i b_i{}^* \in \epsilon(\Lambda_B)\, B^*;$$

so

$$\epsilon(\Lambda_A)\, A^* \subset \epsilon(\Lambda_B)\, B^*.$$

Since H is semisimple, $\epsilon(\Lambda_A)$ and $\epsilon(\Lambda_B)$ are nonzero. Since $\epsilon(\Lambda_A)\, A^* = ((1/\epsilon(\Lambda_A))A)^*$ and $\epsilon(\Lambda_B)\, B^* = ((1/\epsilon(\Lambda_B))B)^*$,

$$((1/\epsilon(\Lambda_A))A)^* \subset ((1/\epsilon(\Lambda_B))B)^*.$$

This implies

$$(1/\epsilon(\Lambda_A))A \supset (1/\epsilon(\Lambda_B))B.$$

Therefore,

$$\epsilon(L_B)A = \epsilon(\Lambda_B)A \supset \epsilon(\Lambda_A)B = \epsilon(L_A)B, \qquad \text{Q.E.D.}$$

COROLLARY 3.2. *Let R be a Dedekind domain with quotient field F, and let H be a finite-dimensional semisimple Hopf algebra over F. If A and B are R-orders in H with $A \subset B$ and $\epsilon(L_A) = \epsilon(L_B)$, then $A = B$.*

4. The Degrees of Irreducible Representations

In this section, we prove a result which is essentially a straightforward generalization to Hopf algebras of Frobenius' theorem that the degrees of the irreducible representations of a finite group divide the order of the group. However, because of the possibility of using Hopf algebra orders in group algebras which are larger than the group ring, this result includes not only Frobenius' theorem, but also Ito's generalization of it, which asserts that the degrees divide the index of any normal abelian subgroup. We then use the result to prove that a separable involutory Hopf algebra over the ring of algebraic integers in a number field is commutative.

LEMMA 4.1. *Let H be a finite-dimensional semisimple involutory Hopf algebra which is split over the field F, let Λ be a left integral in H, and let χ be an irreducible character of H. Then*

$$\gamma(\chi) > \Lambda = (\epsilon(\Lambda)/d_\chi)\, e_\chi\,,$$

where d_χ denotes the degree of the character χ, and e_χ denotes the central idempotent associated with χ.

Proof. Let $\{a_{ij}^*\}$ be a matric basis of the simple subcoalgebra of H^* associated with χ, and let $\{b_{ij}^*\}$ be a matric basis of any other simple subcoalgebra of H^*. Then $\chi = \sum_k a_{kk}^*$, and so by (3.6) Corollary of [4],

$$\begin{aligned} a_{ij}^*(\gamma(\chi) > \Lambda) &= \Big(\sum_k a_{ij}^* \gamma(a_{kk}^*)\Big)(\Lambda) \\ &= (\epsilon(\Lambda)/d_\chi)\, \delta_{ij} \end{aligned}$$

and

$$b_{ij}^*(\gamma(\chi) > \Lambda) = \Big(\sum_k b_{ij}^* \gamma(a_{kk}^*)\Big)(\Lambda) = 0.$$

This implies that $\gamma(\chi) > \Lambda = (\epsilon(\Lambda)/d_\chi) \sum_k e_{kk}$, where $\{e_{ij}\}$ is the basis of matrix units dual to the matric basis $\{a_{ij}^*\}$. This completes the proof of the Lemma.

PROPOSITION 4.2. *Let R be a Dedekind domain with field of quotients F, and let H be a finite-dimensional semisimple involutory Hopf algebra which is split over F. Let A be an R-order in H, and let L denote the ideal of left integrals in A. Then for any irreducible character χ, the ideal $d_\chi R$ divides the ideal $\epsilon(L)$, where d_χ denotes the degree of the character χ.*

Proof. As before, we may assume that R is a discrete valuation ring. Let

Λ be a nonsingular left integral in A. Then $L = R\Lambda$, so $\epsilon(L) = \epsilon(\Lambda)R$. Let V be the simple H-module associated with χ, and let $v \in V$ be any nonzero element. Then Av is a lattice in V. Taking an R-basis of Av as an F-basis of V, and computing the trace with respect to this basis, we see that $\chi(a) \in R$ for all $a \in A$, i.e., $\chi \in A^*$. This implies that $f = \gamma(\chi) > \Lambda \in A$. From Lemma 4.1, $f^n = (\epsilon(\Lambda)/d_\chi)^{n-1}f$. Since the submodule $\sum Rf^n \subset A$ must be finitely generated, it follows that $\epsilon(\Lambda)/d_\chi \in R$. This completes the proof of the proposition.

Let G be a finite group, let F be an algebraic number field which splits G, and let R be the ring of algebraic integers in F. Let $H = FG$. If $A = RG$, then $\Lambda = \sum g$ is a nonsingular left integral in A and $\epsilon(\Lambda) = | G |$. Therefore, in this case, the proposition gives us Frobenius' theorem that the degree of an irreducible representation divides the order of the group. By choosing Λ more carefully we can get Ito's generalization of Frobenius' theorem:

COROLLARY 4.3. *Let G be a finite group, let N be a normal abelian subgroup of G, and let V be an absolutely irreducible representation of G over an algebraic number field F. Then* $\dim_F V$ *divides* $[G : N]$.

Proof. By replacing F by a finite extension, if necessary, we may assume that G and N are split over F. Let R be the ring of integers in F. Since N is abelian and split over F, $FN = \Sigma \oplus F$ as algebras so $FN^* \cong FK$ for some group K. (Of course, $K \cong N$, but we do not need this fact.) Therefore $FN \cong FK^*$. This implies that RK^* is an R-order in FN. Let $A = RG \cdot RK^* \subset FG$. It is clear that A is a finitely-generated projective R-module. Since RK is mapped onto itself by each Hopf algebra automorphism of FK, it follows that RK^* is mapped onto itself by each Hopf algebra automorphism of FN. In particular, if $g \in G$, the map $b \mapsto b^g = g^{-1}bg$, $b \in FN$, is a Hopf algebra automorphism. Therefore if $b \in RK^*$, then $b^g \in RK^*$. Since $bg = gb^g$ for any $g \in G$, $b \in RK^*$, $RK^* \cdot RG \subset RG \cdot RK^*$. This implies that A is an R-subalgebra of FG. If $a \in RG$, $b \in RK^*$, then $\delta(ab) = \sum a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)} \in A \otimes_R A$. This proves that A is an R-order in FG.

In RK^*, the function Λ' defined by $\Lambda'(1) = 1$ and $\Lambda'(k) = 0$ if $k \neq 1$ is a nonsingular left integral. Thought of as an element of FN, $\Lambda' = | N |^{-1} \sum n$. Therefore $\Lambda'' = | N |^{-1} \sum g = (\sum g_i)(| N |^{-1} \sum n)$, where $\{g_i\}$ is a set of coset representatives of N in G, is a left integral in A. Note that $\epsilon(\Lambda'') = [G : N]$. Let L denote the ideal of left integrals in A. Since $\Lambda'' \in L$, $\epsilon(L)$ divides $\epsilon(\Lambda'')R = [G : N]R$. By the proposition, $(\dim_F V)R$ divides $\epsilon(L)$. Therefore $\dim_F V$ divides $[G : N]$. This completes the proof of the corollary.

PROPOSITION 4.4. *Let F be a number field, and let R be the ring of algebraic* *integers in F. If A is a separable involutory Hopf algebra over R, then A is commutative.*

Proof. Let $H = A \otimes_R F$. H is a semisimple Hopf algebra. Let E be a finite extension of F which splits H, and let S be the ring of algebraic integers in E. Note that $A \otimes_R S$ is separable. Therefore, by Proposition 2.5, $\epsilon(L) = S$, where L is the ideal of left integrals in $A \otimes_R S$. Applying Proposition 4.2, we conclude that d_χ is a unit in S for all irreducible characters χ of $A \otimes_R E$, so $d_\chi = 1$. This implies that A is commutative. Q.E.D.

References

1. M. Auslander and O. Goldman, The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.* **97** (1960), 367–409.
2. R. G. Larson, Group rings over Dedekind domains. I, *J. Algebra* **5** (1967), 358–361.
3. R. G. Larson, Group rings over Dedekind domains. II, *J. Algebra* **7** (1967), 278–279.
4. R. G. Larson, Characters of Hopf algebras, *J. Algebra* **17** (1971), 352–368.
5. R. G. Larson and M. E. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–94.
6. M. E. Sweedler, Integrals for Hopf algebras, *Ann. of Math.* (2) **89** (1969), 323–335.
7. M. E. Sweedler, "Hopf Algebras," Benjamin, New York, 1969.